

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

IN RE SUBPOENAS SERVED ON
LLOYDS BANKING GROUP PLC;
LLOYDS AMERICA SECURITIES
CORPORATION; LLOYDS BANK
CORPORATE MARKETS PLC; THE
CANADIAN IMPERIAL BANK OF
COMMERCE; CIBC BANK U.S.A.; BANK
OF AMERICA CORPORATION; BANK OF
AMERICA, N.A.; WELLS FARGO &
COMPANY; WELLS FARGO BANK, N.A.;
THE GOLDMAN SACHS GROUP, INC.;
GOLDMAN SACHS & CO. LLC;
GOLDMAN SACHS INTERNATIONAL;
MORGAN STANLEY; MORGAN
STANLEY & CO. LLC; MORGAN
STANLEY & CO. INTERNATIONAL PLC;
MIZUHO BANK, LTD.; MIZUHO
AMERICAS LLC; MIZUHO SECURITIES
USA LLC; CRÉDIT AGRICOLE CIB;
CREDIT AGRICOLE SECURITIES (USA)
INC.; CREDIT AGRICOLE AMERICA
SERVICES, INC.; SOCIÉTÉ GÉNÉRALE
S.A.; SG AMERICAS SECURITIES, LLC;
BANCO SANTANDER, S.A.; AND
SANTANDER HOLDINGS USA, INC.:

UKRAINE,

Petitioner,

-against-

PAO TATNEFT,

Respondent.

Misc. Case No. 1:21-mc-00376-JGK-SN

(Arising from Case No. 1:17-cv-00582-CKK
in the United States District Court for the
District of Columbia,
pending on appeal in Case No. 20-7091 in the
United States Court of Appeals for the
District of Columbia Circuit)

UKRAINE'S MOTION FOR PROTECTIVE ORDER

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. UKRAINE’S INTERESTS DESERVING OF PROTECTION	2
III. THE PROTECTIVE ORDER THAT UKRAINE SEEKS IS SUPPORTED BY GOOD CAUSE	6
A. Ukraine’s “Classified Defense Information” should not be disclosed in the face of a serious threat of Russian invasion.....	9
B. Ukraine’s “Classified Information” deserves the same treatment routinely afforded to the United States’ classified information	12
C. Designation and treatment of “Attorney Eyes Only” information should account for the heightened sensitivity of certain discovery materials.....	13
D. Designation and treatment of “Confidential Information” should account for the interests of Ukraine and the relevant account holders	15
E. Rule 69 does not authorize handover of information to Russia.....	19
F. Rule 69 authorizes discovery only for use in proceedings to enforce the underlying D.C. District Court judgment	21
IV. CONCLUSION.....	22

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apex Oil Co. v. DiMauro</i> , 110 F.R.D. 490 (S.D.N.Y. 1985)	7
<i>Duling v. Gristede’s Operating Corp.</i> , 266 F.R.D. 66 (S.D.N.Y. 2010)	6
<i>Halkin v. Helms</i> , 690 F.2d 977 (D.C. Cir. 1982)	6
<i>In re Terrorist Bombings of U.S. Embassies in E. Afr.</i> , 552 F.3d 93 (2d Cir. 2008)	13
<i>In re The City of New York</i> , 607 F.3d 923 (2d Cir. 2010)	13
<i>In re von Bulow</i> , 828 F.2d 94 (2d Cir. 1987)	16, 23, 24
<i>United States v. Aref</i> , 533 F.3d 72 (2d Cir. 2008)	9
<i>Zuckerbraun v. Gen. Dynamics Corp.</i> , 935 F.2d 544 (2d Cir. 1991)	10, 13
<i>Zwack v. Kraus Bros. & Co.</i> , 237 F.2d 255 (2d Cir. 1956)	20
Protective Orders	
<i>Flatow v. Iran</i> , 1:97-cv-00396 (D.D.C. Mar. 15, 2001), No. 162	1, 17, 18, 22
<i>Gates v. Syrian Arab Republic</i> , 1:11-cv-08715 (N.D. Il. Mar. 5, 2012), No. 72	21
<i>NML v. Argentina</i> , 06-cv-6466 (S.D.N.Y. Sept. 11, 2008), No. 105	1, 14, 18
<i>Owens v. Sudan</i> , 1:01-cv-02244 (D.D.C. July 8, 2019), No. 436	18
<i>Owens v. Sudan</i> , 1:01-cv-02244 (D.D.C. Apr. 29, 2019), No. 432	16, 17, 18
<i>Owens v. Sudan</i> , 1:01-cv-02244 (D.D.C. June 17, 2010), Dkt. 184	13

Statutes

18 U.S.C. App. 3 § 4	4, 11
----------------------------	-------

Other Authorities

Fed. R. Civ. P. 7	25
-------------------------	----

Fed. R. Civ. P. 26	1, 12, 8
--------------------------	----------

Fed. R. Civ. P. 69	8, 21, 23, 24
--------------------------	---------------

Other Sources

Joseph Biden Jr., “Remarks by President Biden in Press Conference,” (Jan. 19, 2022)	5
---	---

National Security Agency, “NSA, Partners Release Cybersecurity Advisory on Brute Force Global Cyber Campaign” (Jul. 1, 2021)	6, 12
--	-------

Patrick Howell O’Neill, “The \$1 billion Russian cyber company that the US says hacks for Moscow” (Apr. 15, 2021)	22
---	----

Tatneft, “Board of Directors” (last accessed Jan. 21, 2022)	6, 22
---	-------

I. INTRODUCTION

Pursuant to Federal Rule of Civil Procedure 26(c), the District Court’s order of November 26, 2021 (Dkt. 27), and this Court’s order of December 10, 2021 (Dkt. 32), Ukraine respectfully moves for entry of the attached proposed protective order. The District Court remanded “for consideration of an appropriate protective order” to address “the various interests asserted by Ukraine.” Dkt. 27 at 16. Since that time, the strength of Ukraine’s interest in protecting information that could be used to undermine its economic and physical security has only become more vital. Russia has “grown more insistent that Ukraine is fundamentally a part of Russia,” mobilized about 100,000 troops near Ukraine’s border, and prepared a plan for a massive invasion of Ukraine. Markarova Decl. ¶¶ 13–14. In tandem with its military plans, Russia has also developed plans “to destabilize Ukraine from within.” *Id.* ¶ 14.

Without forfeiting any arguments on appeal,¹ Ukraine submits that its economic and physical security cannot be adequately safeguarded without, at the very least, the protections in Ukraine’s proposed order. These protections are similar to those in other cases involving discovery from sovereign nations, including the United States, and Ukraine is seeking them simultaneously in the D.C. District Court. *See, e.g.,* Protective Order, *Owens v. Sudan*, 1:01-cv-02244 (D.D.C. July 8, 2019); Stipulated Protective Order, *NML v. Argentina*, 06-cv-6466 (S.D.N.Y. Sept. 11, 2008); *Flatow v. Iran*, 1:97-cv-00396 (D.D.C. Mar. 15, 2001); *cf.* 18 U.S.C. App. 3 § 4.

¹ For example, this motion should not be construed as an admission that Tatneft is entitled to the sweeping discovery it has requested or that any protective order can adequately protect the interests asserted by Ukraine. Because these issues are pending on appeal before the Second Circuit and are inextricably intertwined with the issues presented by a disputed protective order, Ukraine respectfully submits that there is a substantial question whether the Court has subject matter jurisdiction to enter a protective order pending appeal. *See* Dkt. 29.

II. UKRAINE’S INTERESTS DESERVING OF PROTECTION

On November 26, 2021, the District Court remanded Ukraine’s Motion to Quash with instructions that “the various interests asserted by Ukraine could be handled with an appropriate protective order.” Dkt. 27 at 16. In its Motion to Quash, Ukraine had asserted that concerns for the nation’s economic and physical security gave it interests in “the confidentiality of information about its assets and the assets of related but distinct entities that enjoy sovereign immunity,” “in compliance with its laws and treaties,” and “in confidentiality of sensitive information about the financial affairs of Ukraine and third parties of strategic importance to the nation’s welfare.” Dkt. 12 at 4–8.

As Ukraine explained, these interests “are particularly strong where, as here, discovery is sought by a party with close ties to a hostile state.” *Id.* at 4. For example, Tatneft’s Chairman of the Board is the President of Tatarstan, a political subdivision of the Russian Federation.² Other board members include two Assistants to the President, the Minister of Finance, the Minister of Land and Property Relations, and the Head of the State Legal Administration. *Id.* Thus, a disclosure to Tatneft is a disclosure to Government officials who are in Tatneft’s leadership. Tatarstan retains a substantial ownership interest in Tatneft, including a golden share that allows it to veto important decisions, and has so much influence that it has even used Tatneft’s assets to raise funds for its own use.³ And Tatneft’s Advisor to the General Director on International Legal Matters, who has represented Tatneft in the litigation and arbitration in this very case, also represents the Republic of Tatarstan, a political subdivision of the Russian Federation, in a parallel case and is a member of the Advisory Council on International Law of the Ministry of Justice of

² “Board of Directors,” Tatneft, <https://www.tatneft.ru/for-shareholders/control-and-management-system/board-of-directors/?lang=en> (last accessed Jan. 21, 2022).

³ OAO Tatneft v. Ukraine, PCA Case No. 2008-8, Partial Award on Jurisdiction, ¶¶ 43, 129, 141.

the Russian Federation. *See* Dkt. 12-11 (confirming the individual is Advisor to Tatneft’s General Director on International Legal Matters); Dkt. 12-12 ¶ 43 (confirming the individual attended PCA arbitration merits hearing on behalf of PAO Tatneft as a party representative); Dkt. 12-13 ¶ 3.3(a)(xii) (confirming the individual attended PCA arbitration merits hearing on behalf of the Republic of Tatarstan and/or its Ministry of Land and Property Relations); Ex. A (identifying same individual as “the client,” that is, the Republic of Tatarstan and/or its Ministry of Land and Property Relations, for purposes of requesting a summons to attend a hearing at the Paris Court of Appeal); Dkt. 12-10 (confirming the individual is on the Advisory Council on International Law of the Ministry of Justice of the Russian Federation).⁴

These ties have grown even more concerning in the face of escalating Russian threats to Ukraine’s national security, which have been acknowledged by the U.S. executive branch. In December 2021, U.S. Undersecretary of State for Political Affairs Victoria Nuland warned the Senate that Russia was positioning itself “to destabilize Ukraine from within” as well as “to act decisively in Ukraine when ordered to do so, potentially in early 2022. The intended force, if fully mobilized, would be twice the size of what we saw last spring, including approximately 100 Battalion Tactical Groups (BTGs), or nearly all of Russia’s ready ground forces based West of the Urals.” Markarova Decl. ¶¶ 14–15. In January 2022, the United States “disclosed intelligence showing that Russia has a war plan envisioning an invasion force of 175,000 troops.” *Id.* ¶ 17. Ukraine was subjected to a massive cyber-attack, which a U.S. diplomat recognized as a “tried and true part of the Russian playbook,” consistent with past Russian efforts “to destabilise

⁴ As has previously been noted, participation in the Advisory Council does not make this attorney a Russian government official, but does indicate that he comes in contact with such officials, who could subtly or overtly ply him for information that—even if seemingly innocuous or shared inadvertently—would undermine Ukraine’s interests.

governments, to test their own capabilities, to undercut the sense of confidence of governments that they have gripes with.” *Id.* In a recent security alert, the U.S. Embassy in Kyiv noted “[c]oncerning reports of further unusual Russian military activity near Ukraine’s borders and in occupied Crimea” and warned that “the security conditions may change with little or no notice.” *Id.* ¶ 18. Just two days ago, President Biden stated, “My guess is he [Putin] will move in” on Ukraine.⁵

To facilitate its aggression, “Russia proactively seeks to obtain sensitive information concerning Ukraine’s national security and when obtained routinely uses that information against Ukraine.” Reznikov Decl. ¶ 15. “Russia proactively has targeted information like that requested by Tatneft in a variety of ways, including by offering positive and negative incentives to encourage private individuals and companies to share information and by hacking private individuals and companies in whom Ukraine has confided.” *Id.* Moreover, the U.S. National Security Agency has publicly disclosed that Russian military intelligence is known to target law firms in information-gathering cyber-attacks, and it is hardly to be expected that Tatneft’s counsel will not receive similar attention if known to possess a central repository of Ukraine’s state secrets concerning national defense.⁶

While Ukraine recognizes the determinations of the Arbitral Tribunal and this Court that Tatneft and Russia are legally distinct entities, Ukraine remains acutely concerned that the undisputedly close ties between Tatneft and the State will make it susceptible to a leak. “[I]t is

⁵ Joseph Biden Jr., “Remarks by President Biden in Press Conference,” (Jan. 19, 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/19/remarks-by-president-biden-in-press-conference-6/> (last accessed Jan. 21, 2022).

⁶ National Security Agency, “NSA, Partners Release Cybersecurity Advisory on Brute Force Global Cyber Campaign” (July 1, 2021) (available at <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2677750/nsa-partners-release-cybersecurity-advisory-on-brute-force-global-cyber-campaign/>) (last accessed January 21, 2022).

extraordinarily difficult to identify the source of a leak. It is difficult to prove forensically how common it is for the Russian Federation to obtain information from a Russian company or a U.S. law firm using positive incentives, negative incentives, or cyber-attacks.” Reznikov Decl. ¶ 16. However, the Minister of Defense, who has deep experience in evaluating security questions, has declared, “Based on the evidence and information that is available to me as the Minister of Defense of Ukraine and member of the Military Cabinet of the National Security and Defense Council of Ukraine, there is a very practical and realistic threat that information provided to Tatneft, or even to Tatneft’s outside counsel in the United States, will find its way into the hands of the Russian Federation and where it will be used to undermine Ukraine national security and defense.” *Id.* ¶¶ 16–18.

In this context, Ukraine has significant concern over the sweeping discovery about Ukraine and numerous third parties that Tatneft seeks to obtain through third-party subpoenas allegedly issued in aid of execution of a D.C. District Court judgment confirming an arbitral award. Ukraine’s Ambassador the United States recently warned that disclosure of the information requested by Tatneft “will be extremely harmful to Ukraine’s national security interests and defense, especially given Russia’s historic pattern of aggression toward Ukraine and the recent escalation of its threatening behavior.” Markarova Decl. ¶ 8. Similarly, Ukraine’s Minister of Defense has advised that disclosure of the information requested by Tatneft “will inevitably cause extreme and irreparable harm to Ukraine’s national security,” with a “magnitude and far-reaching implications [that] cannot be overestimated.” Reznikov Decl. ¶ 6. More specifically, he warned:

Should the requested information in response to PAO Tatneft’s discovery requests and subpoenas fall into the hands of an adversary . . . it will no doubt be used to evaluate Ukraine’s defense capabilities with the view to identify vulnerabilities, to plan offensive measures that account for Ukraine’s defense capabilities and exploit its weaknesses, and to interfere with Ukraine’s peaceful

efforts to sustain its interests in the sphere of national defense and territorial integrity, including by identifying, intimidating, and harming companies and individuals, including soldiers, intelligence agents, and informants, with important roles in Ukraine's national defense.

Id. ¶ 10. Both officials have shared a concern that Tatneft's discovery may be "driven by a more far-reaching interstate agenda" than is immediately apparent. *Id.* ¶ 43; Markarova Decl. ¶ 19.

Yet Tatneft has refused to accommodate Ukraine's concerns and interests. To the contrary, it dismissed as unreasonable and excessive even Ukraine's requested stipulation that sensitive discovery materials should not be provided to Russia and should be limited to use in aid of execution of the D.C. District Court's judgment. *Compare* Dkt. 29-2 at 3–4 (proposing that sensitive discovery materials should not be provided to Russia and should be limited to the purposes of Rule 69) *with* Dkt. 29-3 at 2 (stating that the terms proposed by Ukraine include "requests that plainly exceed what is reasonably necessary under the circumstances," attaching a counter-proposal that included no corollary provisions, and claiming, "to the extent your suggestions are reasonable (and consistent with the prior orders in this case) we have incorporated them").

When the parties reported that they were unable to agree on the terms of a stipulated protective order, the Court ordered Ukraine to submit its motion for a protective order by January 21, 2022.

III. THE PROTECTIVE ORDER THAT UKRAINE SEEKS IS SUPPORTED BY GOOD CAUSE

A protective order may be entered upon a showing for "good cause." Fed. R. Civ. P. 26(c). "Good cause is established by 'demonstrating a particular need for protection.'" *Duling v. Gristede's Operating Corp.*, 266 F.R.D. 66, 71 (S.D.N.Y. 2010). Once the moving party provides "the court with information from which it can reasonably conclude that the nature and magnitude

of the moving party's interest are such that protective intervention by the court is justified," the court "weighs the interest of both sides." *Id.* It determines what specific protective measures are most appropriate by balancing "the litigation needs of the discovering party and any countervailing protectible interests of the party from whom discovery is sought." *Apex Oil Co. v. DiMauro*, 110 F.R.D. 490, 496 (S.D.N.Y. 1985) (collecting cases).

It is undisputed between the parties that a protective order is necessary and appropriate under Rule 26 and the order of the District Court to address Ukraine's interests in the protection of sensitive information subpoenaed by Tatneft. The parties differ only as to what substantive protections would be appropriate. Tatneft has not explained how it would be prejudiced by any specific provision proposed by Ukraine, and Ukraine has made a strong showing of the harm it faces absent these provisions. Ukraine's proposal is that four levels of protection be available to four categories of sensitive information.

First, "Classified Defense Information" would be defined as "non-public information concerning Ukraine's military, defense, or intelligence or concerning key players in related industries, including but not limited to SC Ukroboronprom, SE Ukrkosmos, SE Ukrainian Aviation and Transport Enterprise, and State Aviation Enterprises Ukraine, that satisfies the criteria for state secrets under Ukrainian law and the disclosure of which would undermine the national security of Ukraine." Proposed Order § 1.8. The Designating Party would be required to "provide an affidavit explaining the basis for each designation in as much reasonable detail as possible consistent with the national defense interests that the designation is made to protect" *en lieu* of disclosing such information. *Id.* at §§ 4.3(c), 6.2.

Second, "Classified Information" would be defined as "non-public governmental, regulatory, diplomatic, or consular information that is entitled to the highest level of protection

because it satisfies the criteria for state secrets under Ukrainian law.” *Id.* at § 1.7. Unless otherwise ordered by the Court or permitted in writing by the Designating Party,” such information could be disclosed only to (a) individuals who have passed a background check to be conducted by Ukraine or its designee; and (b) U.S. courts and court personnel involved in Enforcement Proceedings. *Id.* at § 6.3; *see also id.* at § 1.15 (defining Enforcement Proceedings to mean “any court proceedings to enforce the January 11, 2021 judgment of the D.C. District Court in Case No. 1:17-cv-00582”).

Third, “Attorney Eyes Only Information” would be defined as “all Discovery Material that contains non-public business, commercial, financial, trade-secret, personal, governmental, regulatory, diplomatic, consular, or national-security related information that is entitled to a higher level of protection due to its heightened sensitivity.” *Id.* at § 1.6. Unless otherwise ordered by the Court or permitted in writing by the Designating Party, such information could be disclosed only to (a) any person authorized to access Classified Information; (b) courts and court personnel involved in Enforcement Proceedings; (c) counsel for Tatneft who appeared in the above-captioned case prior to January 21, 2022; (d) court reporters and/or videographers in Enforcement Proceedings; (e) vendors, experts, and/or consultants to whom disclosure is reasonably necessary for this litigation; and (f) the authors, addressees, or recipients of the document, or any other natural person who would have likely reviewed such document during his or her employment as a result of the substantive nature of his or her employment position. *Id.* at § 6.4.

Fourth, “Confidential Information” would be defined as “all Discovery Material that contains non-public business, commercial, financial, trade-secret, personal, governmental, regulatory, diplomatic, consular, or national-security related information that is entitled to protection due to its sensitivity.” *Id.* at § 1.5. Unless otherwise ordered by the Court or permitted in writing by the Designating Party, such information could be disclosed only to (a) any person

authorized to access Attorney Eyes Only Information; (b) any attorneys and staff who work for a law firm of record in Enforcement Proceedings and are directly participating in that proceeding; (c) officers and employees of Tatneft who are directly supervising or directly participating in Enforcement Proceedings and are not current or former Government officials; (d) former officers, directors, and employees of corporate Parties to whom disclosure is reasonably necessary for this litigation and who are not current or former Government officials; (e) deposition witnesses, but only during their depositions, and in house legal personnel of a Party attending the deposition of a current or former employee; and (f) witnesses, and their Counsel, to the extent necessary to prepare and examine such witnesses. *Id.* at § 6.5.

A. Ukraine’s “Classified Defense Information” should not be disclosed in the face of a serious threat of Russian invasion

Under “venerable” common law principles, the government may “withhold information from discovery when disclosure would be inimical to national security.” *United States v. Aref*, 533 F.3d 72, 79 (2d Cir. 2008). Even in the criminal context, with its heightened constitutional concerns, “[t]he court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure.” 18 U.S.C. App. 3 § 4. And in the civil context, a protective order may recognize the interests of a party or person by “forbidding the disclosure or discovery.” Fed. R. Civ. P. 26(c)(1)(A).

Although this question is inextricably intertwined with Ukraine’s pending appeal, Russia’s massing of military forces on Ukraine’s border and the revelation that Russia has developed a plan for a massive invasion of Ukraine makes the dissemination of state secrets concerning national defense completely inimical to Ukraine’s national security. There are many ways for Russia to obtain sensitive discovery material despite a protective order. A leak to Russia requires only one

individual's cooperation, with or without the knowledge or approval of Tatneft's management. Even purely "internal" Tatneft communications will be able to reach the Russian government through the government officials placed in management. And Russia is known to coerce private companies to provide intelligence. Reznikov Decl. ¶ 15. In addition, Russian military intelligence is known to target law firms for information-gathering cyberattacks.⁷ Given Russia's proactive efforts to gather intelligence about Ukraine, it can be expected to target Tatneft's counsel if Tatneft's counsel is known to possess state secrets on national defense. *See* Reznikov Decl. ¶ 15.

In this context, disclosure of state secrets concerning national defense would be inimical to Ukraine's national security. Ukraine's interest in national security far outweighs any prejudice to Tatneft that may result from limited withholdings of such information while other discovery moves forward. *Cf. Zuckerbraun v. Gen. Dynamics Corp.*, 935 F.2d 544, 547 (2d Cir. 1991) (noting that national security interests justify even "drastic" consequences including dismissal). Tatneft's requests include within their scope state secrets in the field of defense, which Ukrainian law defines to include information "on the content of strategic and operational plans and other documents of military command, preparation and conduct of military operations, strategic and mobilization deployment of troops, as well as other important indicators characterizing the organization, strength, deployment, combat and mobilization readiness, combat and other military training, weapons and other material and technical means of the Armed Forces of Ukraine and other military formations." DDC Dkt. 81-3, Law of Ukraine No. 3855-XII, "On State Secrecy" of 21 January 1994, art. 8(1)(1).⁸

⁷ National Security Agency, "NSA, Partners Release Cybersecurity Advisory on Brute Force Global Cyber Campaign" (Jul. 1, 2021) (available at <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2677750/nsa-partners-release-cybersecurity-advisory-on-brute-force-global-cyber-campaign/>) (last accessed Jan. 21, 2022).

⁸ "DDC Dkt." citations are to the docket in the D.C. District Court case *PAO Tatneft v. Ukraine* (1:17-cv-00582).

For example, a full response to Documents Requests 1 through 3 would include “the extent of Ukraine’s military funding and expenditures, account information for every person or company that has been the recipient of Ukrainian military and defense spending and receivables under the supply contract, including personnel suppliers of military and defense equipment and technology, and the dates and amounts of all such payments.” Reznikov Decl. ¶¶ 8(b), 8(c). “This would shed light on Ukraine’s defense capabilities and disclose the entire network of companies and individuals involved in supporting Ukraine’s national defense, including substantial amounts of non-public information, thereby posing a real danger to Ukraine’s military, state and national intelligence security.” *Id.* at ¶ 8(c).

Moreover, Tatneft’s expansive definition of “Ukraine” means that a full response to its discovery requests would also include “sensitive, non-public information about the assets, financial health, and economic vulnerabilities of key players with roles related to Ukraine’s national defense,” such as “SC Ukroboronprom, a strategic manufacturer of weapons and military hardware in Ukraine consolidating enterprises in the strategic sectors of Ukraine’s national defense industry, SE Ukrkosmos, which maintains satellite communications in Ukraine that are necessary to gather intelligence and to coordinate movements of military personnel and supplies, SE Ukrainian Aviation and Transport Enterprise, an enterprise owning dozens of helicopters forming a unified aviation security and protection system in Ukraine that are also used to patrol Ukraine’s state borders, and State Aviation Enterprise Ukraine, an enterprise owning a helicopter and aircrafts used to fly by senior-level governmental officials and [the] President of Ukraine.” *Id.* ¶¶ 8–9.

Thus, there is good cause for the protective order to permit “non-public information concerning Ukraine’s military, defense, or intelligence or concerning key players in related

industries, including but not limited to SC Ukroboronprom, SE Ukrkosmos, SE Ukrainian Aviation and Transport Enterprise, and State Aviation Enterprises Ukraine, that satisfies the criteria for state secrets under Ukrainian law and the disclosure of which would undermine the national security of Ukraine” to be designated as Classified Defense Information. *See* Proposed Order § 1.8. Such information should not be disclosed in discovery. *See id.* § 6.2. Instead, an affidavit should be provided “explaining the basis for each designation in as much detail as possible consistent with the national defense interests that the designation is made to protect.” *See id.* § 4.3(c).

B. Ukraine’s “Classified Information” deserves the same treatment routinely afforded to the United States’ classified information.

State secrets are the Ukrainian corollary to classified information in the United States. Ukrainian law defines state secrets as “information in the field of defence, economics, science and technology, foreign relations, state security and protection of legal order, the disclosure of which may cause damage to the national security of Ukraine, and which is recognized in the manner prescribed by this Law, as a state secret and subject to state protection.” DDC Dkt. 81-3, Law of Ukraine No. 3855-XII, “On State Secrecy” of 21 January 1994, art. 1(1). A full answer to Tatneft’s discovery requests would require disclosure of state secrets and additional sensitive information that is strictly guarded by the Ministry of Defense because it meets the requirements for designation as a state secret, regardless of whether it has yet been formally designated as such. Reznikov Decl. ¶¶ 11–14. It would be appropriate by analogy and in the interests of comity for a protective order in this case to provide that Ukraine’s state secrets be accorded, at the very least, the same treatment as the United States’ classified information.

Discovery in cases involving information classified by the U.S. Government consistently requires a protective order that prohibits “the sharing of classified information with persons not cleared to receive the information by the Executive Branch.” Robert Timothy Reagan,

“Confidential Discovery: A Pocket Guide on Protective Orders,” Federal Judicial Center (2012), 15. Courts have “authority to limit access to classified information to persons with a security clearance.” *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 93, 122 (2d Cir. 2008). In addition, they can provide for discovery material to receive “special treatment as if the document or information were classified, even if the document or information has not been formally deemed to be classified.” Protective Order § 11, *Owens v. Sudan*, 1:01-cv-02244 (D.D.C. June 17, 2010), No. 184; *see also id.* § 15 (providing that even counsel and court reporters “must have been successfully cleared by the FBI and agree, as evidence by their signature, to abide by the terms of the attached MOU and Acknowledgment” before accessing “possibly classified information”).

Similarly, there is good cause in this case to treat as a state secret all information requested by Tatneft that has been formally designated a state secret or that qualifies for such a designation although it has not yet been formally made. The protective order should allow for “non-public governmental, regulatory, diplomatic, or consular information that is entitled to the highest level of protection because it satisfies the criteria for state secrets under Ukrainian law” to be designated as Classified Information. *See* Proposed Order § 1.7. Such information should be disclosed only to “(a) Individuals who have passed a background check to be conducted by Ukraine or its designee; and (b) U.S. courts and court personnel involved in Enforcement Proceedings.” *See id.* § 6.3.

C. Designation and treatment of “Attorney Eyes Only” information should account for the heightened sensitivity of certain discovery materials.

“The disclosure of confidential information on an ‘attorneys’ eyes only’ basis is a routine feature of civil litigation involving trade secrets” and has also been used in criminal cases involving national security information. *In re The City of New York*, 607 F.3d 923, 935 & n.12 (2d Cir. 2010). Tatneft’s requests include non-public information that bears on Ukraine’s physical and

economic security. Moreover, Tatneft’s requests include trade-secret, commercial-secret, and bank-secret information about the accounts, finances, and financial transactions of third parties whose information Ukraine is not at liberty to disclose, including energy companies that compete directly or indirectly with Tatneft and that play an important role in Ukraine’s energy security. *See* Dkt. 2-1 at 2–3 (defining Ukraine to include “Identified State Controlled Entities” including Naftogaz of Ukraine, Naftogaz Trading Europe, Energoatom, Centrenergo, and Electrotiyazhmash); Dkt. 2-2 at 2–3 (same); Mudra Decl. ¶¶ 13, 25.

To adequately protect the interests of Ukraine and other account holders, there is good cause for the protective order to permit the designation of information as “Attorney Eyes Only” if it “contains non-public business, commercial, financial, trade-secret, personal, governmental, regulatory, diplomatic, consular, or national-security related information that is entitled to a higher [than Confidential] level of protection due to its heightened sensitivity.” Proposed Order § 1.6.

Tatneft has mistakenly suggested in the alternative that the second level of confidentiality, which it terms “Highly Confidential Information,” should require “a substantial risk of injury that could not be avoided by less restrictive means.” Dkt. 29-3 at 3. But it has offered no precedent or explanation of its own interests to support this narrow tailoring requirement. *Compare* Stipulated Protective Order § 2(c), *NML v. Argentina*, 06-cv-6466 (S.D.N.Y. Sept. 11, 2008), No. 105 (stipulation, by an attorney now representing Tatneft against Ukraine, and agreement by the Court that “Highly Confidential Information” should include “any trade secret or other confidential financial, commercial, governmental or regulatory information contained in any document or testimony that is entitled to a higher [than Confidential] level of protection due to its heightened sensitivity”). Because the routine practice of designating especially sensitive information for

“Attorney Eyes Only” would further the interests of Ukraine and the account holders without prejudice to Tatneft, there is good cause to allow such designations here.

Tatneft has also suggested that access to information with a heightened confidentiality designation should be provided to witnesses and deposition witnesses, including current or former employees, and to counsel for such witnesses, including in-house counsel. Dkt. 29-3 at 11–12. Especially given the close ties between Tatneft and Russia and the relationship of at least one of Tatneft’s legal advisers with Russia, Ukraine’s interests cannot be adequately protected by an order that provides advance permission to make a disclosure to any witness or in-house counsel of Tatneft’s choosing. Any prejudice to Tatneft in omitting advance authorization is mitigated by the fact that any testimony that would be relevant in a proceeding to enforce the judgment of the D.C. District Court can likely be elicited by authorized outside counsel calling a witness to whom disclosure of Attorney Eyes Only Information is permitted under more targeted provisions of Ukraine’s proposed order. *See* Proposed Order at §§ 6.4(c) (authorizing disclosure to specific outside counsel), (e) (authorizing disclosure to experts), and (f) (authorizing disclosure to “authors, addressees, or recipients of the document, or any other natural person who would have likely reviewed such document during his or her employment as a result of the substantive nature of his or her employment position”); *see also id.* § 6.4 (permitting disclosure of Attorney Eyes Only Information to anyone upon written permission by the Designating Party).

D. Designation and treatment of “Confidential Information” should account for the interests of Ukraine and the relevant account holders.

There is good cause for applying a presumption of confidentiality to all non-public information requested by Tatneft. Non-public information of the type requested by Tatneft could clearly be used, among other things, to interfere with Ukraine’s economic security and to evaluate and capitalize on vulnerabilities in Ukraine’s national defense apparatus. A presumption of

confidentiality would reduce the risk of disclosure to Tatneft—including Russian officials in Tatneft’s management—of information that should have been protected more stringently than Confidential Information. This is important because, once sensitive information has been disclosed, the damage is often irreversible. *See In re von Bulow*, 828 F.2d 94, 99 (2d Cir. 1987) (noting that no judicial remedy can “unsay the confidential information that has been revealed”).

Ukraine is known to be the target of Russian intelligence efforts, and it is difficult to fully anticipate all the ways in which Russian intelligence could take advantage of publicly disclosed discovery materials. “Intelligence gathering is akin to the construction of a mosaic in which thousands of bits and pieces of seemingly innocuous information can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate.” *Halkin v. Helms*, 690 F.2d 977, 993 n.57 (D.C. Cir. 1982) (cleaned up). Thus, even “seemingly innocuous information” may be useful “to a sophisticated intelligence analyst.” *Id.* Moreover, Tatneft’s discovery requests implicate Ukraine’s interest in the confidentiality of non-public information about its monetary policy or the interests of account holders, including Ukraine, in the confidentiality of non-public information about their accounts.

Document Requests 1 through 3 and 6 demand detailed account information belonging to Ukraine and to other third parties,⁹ including current balances, currencies, as-of date, ownership and beneficial ownership interests, signatory rights, and transaction history, including transfers of funds and, more specifically, transfers of funds in connection with securities or bond offerings. Such information is regularly treated as confidential under U.S. law. *See, e.g.*, Order § 2, *Owens v. Sudan*, 1:01-cv-02244 (D.D.C. Apr. 29, 2019), No. 432 (requiring confidential treatment of discovery material produced by third-party subpoena recipient, including sensitive financial

⁹ While Tatneft maintains that these third parties are at least potentially relevant to the judgment against Ukraine, it is undisputed that they are legally distinct from the Government of Ukraine.

information, non-public financial information of any kind, wire transfer information, bank account numbers, and transaction history that would reveal non-public information about Defendant's business counterparts); Consent Protective Order at 1–2, *Flatow v. Iran*, 1:97-cv-00396 (D.D.C. Mar. 15, 2001) (listing federal laws that protect banking information before ordering “a certain degree of confidentiality as to matters such as financial information concerning persons or entities about whom information might be revealed” through discovery provided by the United States). Such information is also protected by Ukrainian bank secrecy law, which is rigorously enforced. Mudra Decl. ¶¶ 6–21, 23–24. This information is not subject to disclosure upon the order of a foreign court, and “Ukraine has no right under Ukrainian bank secrecy law to disclose information of third parties that is included within the scope of Tatneft’s discovery requests and subpoenas.” *Id.* ¶¶ 22, 25. Thus, the relevant account holders have a clear confidentiality interest in non-public information covered by Document Requests 1 through 3 and 6.

Document Requests 4 through 7 include within their scope sensitive, non-public information about Ukraine’s actual or expected participation in the securities and bond markets, which could be used to undermine the success of Ukraine’s monetary policy, thereby jeopardizing Ukraine’s economic security. Ukraine, like the United States, has a strong interest in avoiding public disclosure of its actual or expected participation in the securities and bond markets. *See* Dkt. 12-9 (Reuters report on internal, DOJ, and congressional investigations into leak of Federal Reserve plans to purchase bonds). Even where business transactions are not instruments of monetary policy, courts have recognized that it is appropriate to treat non-public information relating to actual, planned, and proposed business transactions as confidential. *See* Order § 2, *Owens v. Sudan*, 1:01-cv-02244 (D.D.C. Apr. 29, 2019), No. 432.

Thus, to streamline the discovery process and provide clarity to the parties, there is good cause to instruct, “All Discovery Material should be designated by the Producing Party as at least Confidential unless counsel for the Producing Party has determined that the information at issue is publicly available.” *See* Proposed Order § 4.2.

A presumption of confidentiality has been recognized as reasonable in other cases involving the disclosure of non-public information. *See, e.g.* Protective Order § 2, *Owens v. Sudan*, 1:01-cv-02244 (D.D.C. July 8, 2019), Dkt. 436 (establishing presumption that “[a]ll information produced in response to the Subpoena, and any portion thereof, is to be deemed confidential . . .”); Consent Protective Order § 1, *Flatow v. Iran*, 1:97-cv-00396 (D.D.C. Mar. 15, 2001), No. 162 (limiting disclosure of “[a]ny non-public documents produced or made available by OCC in response to Plaintiff’s subpoena”).

Also consistent with other cases, and with the position of Tatneft’s own counsel in another case, Confidential Information should be defined to include “all Discovery Material that contains non-public business, commercial, financial, trade-secret, personal, governmental, regulatory, diplomatic, consular, or national-security related information that is entitled to protection due to its sensitivity.” Proposed Order § 1.5; *see also* Order § 2, *Owens v. Sudan*, 1:01-cv-02244 (D.D.C. Apr. 29, 2019), Dkt. 432 (defining Confidential Information to include any “private or confidential information that requires the protection provided in this Order”); Stipulated Protective Order § 2(b), *NML v. Argentina*, 06-cv-6466 (S.D.N.Y. Sept. 11, 2008), No. 105 (stipulation, by an attorney now representing Tatneft against Ukraine, and agreement by the Court that Confidential Information should include “any trade secret or other confidential financial, commercial, governmental or regulatory information contained in any document or testimony that is entitled to such protection due to its sensitivity”).

Tatneft took the position during meet-and-confer that Confidential Information should be defined to account only for the interests of the Producing Party (that is, the subpoena recipient) in privacy and in avoiding liability for disclosures prohibited by law or by confidentiality obligations. Dkt. 29-3 at 6. But this unusual definition of confidentiality does nothing to further its legitimate litigation interests and is contrary to the District Court’s instruction that the protective order should account for Ukraine’s interests. Dkt. 27 at 16.

To ensure that relevant interests are not overlooked or underestimated, Ukraine and the relevant account holders should have a reasonable opportunity to review and designate discovery materials that a subpoena recipient is unsure how to designate before they are produced to Tatneft. *See* Proposed Order § 4.2. There is good cause to consult the interested parties before it is too late.

E. Rule 69 does not authorize handover of information to Russia.

Federal Rule of Civil Procedure 69, Tatneft’s sole legal basis for seeking post-judgment discovery, does not authorize Tatneft’s handover of the collected intelligence—whether direct, indirect, deliberate, or inadvertent—to inform hostile action by Russia against Ukraine. During meet-and-confer, Ukraine suggested that an appropriate order should expressly prohibit disclosure of protected information “to the Russian Federation or its agents, which the order should define broadly in terms that are reciprocal to the definition of Ukraine on which Tatneft has insisted.” Dkt. 29-2 at 4. Without explaining the reason for its position, Tatneft responded with a proposed order that included no such limitation and with an email stating that it had incorporated all of Ukraine’s suggestions “to the extent your suggestions are reasonable.” Dkt. 29-3 at 2; *see also id.* at 4–20.

Reciprocity and consistency require that an analogous definition be used to define “the Russian Federation” as has been adopted to define “Ukraine.” In the spirit of reciprocity and consistency, the protective order must prohibit disclosure of documents and information to the

Russian Federation defined to include its “agencies, instrumentalities, ministries, political subdivisions, representatives, state controlled entities, alter-egos, and assigns, and all other Persons acting or purporting to act for or on Ukraine’s behalf, whether or not authorized to do so.” Compare Proposed Order § 6.1 with Dkts. 2-1 at 3, 2-2 at 3; *cf. Zwack v. Kraus Bros. & Co.*, 237 F.2d 255, 260 (2d Cir. 1956) (affirming prohibition on disclosure of discovery materials to Hungary).

The reciprocal and consistent definition of the Russian Federation does not require any further justification, other than by reasons by reciprocity and consistency. And an express prohibition of disclosure to Russia is necessitated by the circumstances of this case. *First*, disclosure of sensitive information to Russia would undermine each of the interests asserted by Ukraine. *Second*, the risk of disclosure to Russia is substantiated by publicly available information concerning the close ties between Tatneft and the Government, by the direct participation of Government officials in Tatneft’s management,¹⁰ by Russia’s record of coercing private companies to provide intelligence information,¹¹ and by Tatneft’s refusal to stipulate that it will refrain from such disclosures, Dkt. 29-3 at 4–20.¹² *Third*, Tatneft has not identified any

¹⁰ As noted above, numerous examples are provided by Tatneft’s Board of Directors alone. *See* “Board of Directors,” Tatneft, <https://www.tatneft.ru/for-shareholders/control-and-management-system/board-of-directors/?lang=en> (last accessed Jan. 21, 2022).

¹¹ *See, e.g.*, Patrick Howell O’Neill, “The \$1 billion Russian cyber company that the US says hacks for Moscow” (Apr. 15, 2021) (available at <https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking/>) (last accessed Jan. 21, 2022) (describing intelligence work that Positive Technologies conducted for Russia under an “abusive” relationship in which “the implicit threat for non-cooperation can loom large”).

¹² Tatneft’s repeated observation that it is not currently under U.S. sanctions and that its legal separateness from the State was recognized by the arbitral tribunal and the D.C. District Court does not bear on any of these risk factors. This Court’s prior determination that Ukraine did not demonstrate a sufficient risk of Russia obtaining information from Tatneft to quash the subpoenas presents a closely related question that is currently pending on appeal but does not preclude

countervailing interest of its own that would fall within the purposes of Rule 69 discovery and that would be undermined by a protective order prohibiting disclosures of protected information to Russia.

F. Rule 69 authorizes discovery only for use in proceedings to enforce the underlying D.C. District Court judgment.

Tatneft's discovery requests are made under Federal Rule of Civil Procedure 69, which authorizes discovery "[i]n aid of the judgment or execution." Fed. R. Civ. P. 69(a)(2); *see also* Dkt. 2-1 at 1; Dkt. 2-2 at 1. It is undisputed that the judgment at issue here is the January 11, 2021 judgment of the D.C. District Court in Case No. 1:17-cv-00582. *See, e.g.*, Dkt. 11 at 1 (Tatneft's identification of the judgment it seeks to execute). The term "the judgment" in Rule 69 only includes the relevant U.S. judgment, not the arbitral award or a foreign judgment on the award. The object and purpose of Rule 69 is to aid execution of the U.S. judgment.

Thus, a reasonable and appropriate protective order suited to the purposes of Rule 69 discovery would allow Tatneft to use protected material "only as reasonably necessary in connection with Enforcement Proceedings" related to the *D.C. District Court's judgment*. *See* Proposed Order § 6.1; *cf.* Parties' Joint Stipulated Protective Order at 2–3, *Gates v. Syrian Arab Republic*, 1:11-cv-08715 (N.D. Il. Mar. 5, 2012), No. 72 (limiting use of Confidential Information to actions seeking to enforce the specific U.S. judgment pursuant to which discovery was sought).¹³

When Ukraine made this suggestion, Tatneft responded by insisting without explanation that protected material be made available for use in connection with proceedings to enforce the *arbitral award or any judgment related to that award*. *Compare* Dkt. 29-2 at 3 with Dkt. 29-3 at

Ukraine from presenting further evidence and argument that there is a sufficient risk to enter a protective order.

¹³ *See also* Proposed Order at § 1.15 (defining "Enforcement Proceedings" to include "any court proceedings to enforce the January 11, 2021 judgment of the D.C. District Court in Case No. 1:17-cv-00582").

12. This would include judgments obtained by Tatneft in foreign jurisdictions that allow much more limited discovery than the United States, including awards of foreign litigation costs that have no relation to or counterpart in the judgment of the D.C. District Court. *Cf.* DDC Dkt. 69 at 4–6 (noting cost awards obtained by Tatneft in other jurisdictions). Tatneft purports to seek discovery under Rule 69, which authorizes discovery only to enforce the judgment of the D.C. District Court. Tatneft’s rights under Rule 69 would not be prejudiced by the provision Ukraine has suggested. And its right to use protected information from this discovery process in any other litigation should be determined in that other litigation, as contemplated by Section 7 of Ukraine’s proposed order. *See* Proposed Order § 7; *see also* Dkt. 29-3 at 12–13 (Tatneft’s proposal to the same effect); *cf.* Consent Protective Order § 5, *Flatow v. Iran*, 1:97-cv-00396 (D.D.C. Mar. 15, 2001) (requiring separate proceedings to determine whether a party could use discovery in any other action).

IV. CONCLUSION

For these reasons, Ukraine respectfully requests that the Court enter the proposed protective order attached hereto.¹⁴

¹⁴ Ukraine expressly reserves foreign sovereign immunity from attachment and execution under the FSIA, Vienna Convention on Diplomatic Relations, Vienna Convention on Consular Relations, and all other applicable law.

Dated: January 21, 2022

Respectfully submitted,

s/ Maria Kostytska
Maria Kostytska (New York Bar # 4380101)
Winston & Strawn LLP
68 rue du Faubourg Saint Honoré
Paris 75008, France
(331) 53648282
(331) 53648220 (fax)
MKostystka@winston.com

Kelly A. Librera
Winston & Strawn LLP
200 Park Avenue
New York, NY 10166-4193
(212) 294-4622
(212) 294-4700 (fax)
KLibrera@winston.com

Counsel for Ukraine

CERTIFICATE OF SERVICE

I hereby certify that on this 21st day of January 2022 I caused the foregoing document to be served on counsel for Tatneft through ECF.

s/ Maria Kostytska
Maria Kostytska (New York Bar # 4380101)
Winston & Strawn, LLP
68 rue du Faubourg Saint Honoré
Paris 75008, France
(331) 53648282
(331) 53648220 (fax)

Counsel for Ukraine